**RELAZIONE DI LABORATORIO DI SISTEMI**

Titolo dell’esercitazione

**Sviluppo del programma RSA**

**Obiettivo:** Sviluppo di un programma per la generazione di chiavi pubbliche e private, la codifica e la decodifica per mezzo di essi.

**Studio del Sistema:** Per la creazione del programma in questione, avremo bisogno di alcune conoscenze fondamentali per il suo sviluppo:

***Fase 1:*** *Generazione della chiave pubblica e la chiave privata. TEORIA*

Il processo di generazione delle due chiavi segue 5 passi importanti:

1. Si scelgono 2 numeri primi ***p*** e ***q*** molto grandi (con più di 100 cifre) così da rendere quasi impossibile la fattorizzazione del prodotto.
2. Si calcola il prodotto ***N = p \* q*** che rappresenta il valore del modulo per l’aritmetica modulare.
3. Si calcola ***Ø(N)=(p-1)\*(q-1)*** che rappresenta la funzione di Eulero.
4. Si sceglie un numero detto ***e*** (detto esponente pubblico) più piccolo di ***N*** e primo rispetto a ***Ø(N)*** cioè tale che ***MCD(e, Ø(N)) = 1.***
5. Si calcola il numero d (detto esponente privato) tale che:

***d\*e = 1 (mod N) =*** con ***K*** intero positivo che produce per ***d*** un valore intero.

**Infine le due chiavi saranno costituite dalle seguenti coppie:**

**Chiave pubblica = (e, N)**

**Chiave privata = (d, N)**

**Nota: Ovviamente utilizzeremo delle cifre piccole per far vedere in modo chiaro il funzionamento di tale processo.**

***Fase 2:*** *Processo di cifratura. TEORIA*

La cifratura di un messaggio in chiaro M viene effettuata per mezzo della chiave pubblica usando la seguente trasformazione:

messaggio cifrato = **Me** (mod (**N**))

***Fase 3:*** *Processo di decifratura. TEORIA*

La decifratura si effettuerà per mezzo della chiave privata usando la seguente relazione:

**M** = (messaggio cifrato)**d** (mod (**N**))

**Definizione del piano di simulazione e costruzione del software:** Per lo sviluppo del software incominciamo a sviluppare un algoritmo per ogni fase:

***Fase 1:*** *Generazione della chiave pubblica e la chiave privata. ALGORITMO*

*Inserisco nella variabile* ***p*** *un valore primo;*

*Inserisco nella variabile q un valore primo;*

*Calcolo la variabile N attraverso la moltiplicazione di p e q (N = p \* q);*

*Calcolo la variabile fi attraverso la moltiplicazione di p - 1 e q - 1;*

*Inserisco nella variabile e un valore minore di N e primo rispetto a fi;*

*Inserisco nella variabile k il valore 0;*

*Calcolo la variabile d attraverso un ciclo iterativo:*

*finché d non è intero*

*{*

*calcola d attraverso (fi \* k + 1)/e;*

*incrementa k di 1;*

*}*

*Stampa Chiave pubblica = (e, N);*

*Stampa Chiave privata = (d, N);*

***Fase 2:*** *Processo di cifratura. ALGORITMO*

*Inserisco nella variabile frase il messaggio in chiaro;*

*Metto nell’array lettere ogni lettera della frase;*

*Calcolo la lunghezza della frase e la inserisco in lun;*

*Prendo ogni elemento (lettera) dell’array lettere, lo converto in ASCII e ogni numero lo inserisco nell’array ascii;*

*Prendo ogni codice ASCII dall’array ascii, lo elevo alla e, faccio il modulo N, tutto usando il metodo delle moltiplicazioni successive in modo tale di non causare un overflow sulla macchina;*

*Stampo il messaggio cifrato;*

***Fase 3:*** *Processo di decifratura. ALGORITMO*

*Inserisco nella variabile frasecifrata il messaggio cifrato separato per ogni codice ascii da una virgola;*

*Calcolo la lunghezza della frase cifrata;*

*Prendo ogni codice ASCII e lo elevo alla d, faccio il modulo N, usando sempre il metodo delle moltiplicazioni successive;*

*Converto il codice ASCII decifrato in lettere UNICODE;*

*Stampo le lettere che sarà il nostro messaggio decifrato;*

***PROGRAMMA CREATO IN HTML e JAVASCRIPT***

***Ps. Scusate per le tante cose inutili in più che ho messo;***

***<HTML>***

***<HEAD>***

***<style>***

***body{background: -moz-linear-gradient(top, #71B0FF, #FBD5B6) FIXED;}***

***fieldset{text-align:left; border:solid black 2px; border-radius:10px 20px 20px 20px;}***

***span{font-size:25px;line-height: 50px;}***

***input{font-size:25px;border-radius:20px;border:solid black 1px;background:rgba(255,255,255,0.5);padding-left:10px;}***

***div{font-size:25px;border-radius:25px;border:solid black 1px;background:rgba(0,0,0,0.3);padding:8px;}***

***td{border:solid black 3px;font-size:20px;padding:3px;text-align:center;}***

***</style>***

***<TITLE>Crittografia a chiave asimmetrica - RSA</TITLE>***

***<SCRIPT LANGUAGE="JavaScript">***

***var p, q, n, p1, q1, o, d, e, vd;***

***function calcolo()***

***{***

***p=(f.p.value)\*1***

***q=(f.q.value)\*1***

***if(p!=0 && q!=0 && p>0 && q>0)***

***{***

***<!-- inizio calcolo di n -->***

***n=p\*q***

***document.getElementById("n").innerHTML=n***

***<!-- fine calcolo di n -->***

***<!-- inizio calcolo di eulero -->***

***p1=p-1***

***q1=q-1***

***document.getElementById("pp").innerHTML=p1***

***document.getElementById("qq").innerHTML=q1***

***o=p1\*q1***

***document.getElementById("o").innerHTML=o***

***<!-- fine calcolo di eulero -->***

***}***

***else***

***{***

***document.getElementById("n").innerHTML=0***

***document.getElementById("pp").innerHTML=0***

***document.getElementById("qq").innerHTML=0***

***document.getElementById("o").innerHTML=0***

***}***

***}***

***function calcolad()***

***{***

***var k=1;***

***e=f.e.value***

***vd="<table border STYLE='border-collapse:collapse;'><tr style='width:30px;'><td>k</td><td>d</td></tr>"***

***while(d%1!=0)***

***{***

***d=((o\*k+1)/e)***

***if(d%1==0)***

***{***

***vd+="<tr style='background-color:green;'><td style='width:30px;'>"+k+"</td><td>"+d+"</td></tr>"***

***}***

***else***

***{***

***vd+="<tr style='background-color:red;'><td style='width:30px;'>"+k+"</td><td>"+d+"</td></tr>"***

***}***

***k++***

***}***

***vd+="</table>"***

***document.getElementById("d").innerHTML=vd***

***document.getElementById("se").innerHTML=e***

***document.getElementById("sn1").innerHTML=n***

***document.getElementById("sn2").innerHTML=n***

***document.getElementById("sd").innerHTML=d***

***}***

***var a, b, mo, el;***

***var ar=new Array(), fr, le, ms="", a2, ar2=new Array(), testochiaro=new Array(), tabella="";***

***function pp()***

***{***

***fr=f.m1.value***

***le=fr.length***

***for(var k=0; k<le; k++)***

***{***

***testochiaro[k]=(fr.substring(k,k+1))***

***ar[k]=(fr.substring(k,k+1)).charCodeAt(0)***

***}***

***el=f.em1.value\*1***

***b=f.nm1.value\*1***

***for(var g=0; g<le; g++)***

***{***

***a=ar[g]***

***a2=Math.pow(a,1)%b***

***for(h=2;h<=el;h++)***

***{***

***a2=(a2\*a)%b***

***}***

***ar2[g]=a2***

***}***

***//inizio tabella di riepilogo***

***tabella+="<table border STYLE='border-collapse:collapse;'><tr><td>Testo in chiaro</td>"***

***for(i=0; i<le; i++)***

***{***

***tabella+="<td>"+testochiaro[i]+"</td>"***

***}***

***tabella+="</tr><tr><td>Testo ASCII</td>"***

***for(i=0; i<le; i++)***

***{***

***tabella+="<td>"+ar[i]+"</td>"***

***}***

***tabella+="</tr><tr><td>Testo cifrato</td>"***

***for(i=0; i<le; i++)***

***{***

***tabella+="<td>"+ar2[i]+"</td>"***

***}***

***tabella+="</tr></table>"***

***//fine tabella di riepilogo***

***document.getElementById("pr").innerHTML=tabella+"<br>Copiare per la decifratura: "+ar2***

***}***

***var ar4=new Array(), fr2, ar2, lu2, a2, dl, po2=1, mo2, ndecifrato, mss2="", moo2, ar3=new Array(), a33, h, a22, testoca=new Array();***

***function pd()***

***{***

***fr2=f.m2.value //frase cifrata con le ,***

***ar4=fr2.split(",") //ogni codice lettere in un elemento delll'array ar4***

***lu2=ar4.length //lunghezza array***

***dl=f.dm2.value\*1 // d***

***ndecifrato=f.nm2.value\*1 // n***

***for(var g2=0; g2<lu2; g2++) //scorre tutto l'array***

***{***

***a33=Math.pow(ar4[g2],1)%ndecifrato***

***for(h=2;h<=dl;h++)***

***{***

***a33=(a33\*ar4[g2] )%ndecifrato***

***}***

***ar3[g2]=a33***

***testoca[g2]=String.fromCharCode(a33)***

***}***

***//inizio tabella di riepilogo***

***mss2+="<table border STYLE='border-collapse:collapse;'><tr><td>Testo cifrato</td>"***

***for(i=0; i<le; i++)***

***{***

***mss2+="<td>"+ar4[i]+"</td>"***

***}***

***mss2+="</tr><tr><td>Testo decifrato in ASCII</td>"***

***for(i=0; i<le; i++)***

***{***

***mss2+="<td>"+ar3[i]+"</td>"***

***}***

***mss2+="</tr><tr><td>Testo decifrato in chiaro</td>"***

***for(i=0; i<le; i++)***

***{***

***mss2+="<td>"+testoca[i]+"</td>"***

***}***

***mss2+="</tr></table>"***

***//fine tabella di riepilogo***

***document.getElementById("pr2").innerHTML=mss2***

***}***

***</SCRIPT>***

***</HEAD>***

***<BODY>***

***<CENTER>***

***<h1>Crittografia a chiave asimmetrica - RSA</h1>***

***<h2 style="color:red">Per far sì che il programma funzioni, la <i>d</i> > <i>e</i>, ed <i>N</i> > 100.***

***Cambiare i valori per <i>p</i>, <i>q</i> ed <i>e</i> per soddisfare tale esigenza.</h2>***

***<form name="f">***

***<fieldset>***

***<legend><div>Calcolo delle chiavi</div></legend>***

***<span>***

***Inserisci <i>p</i>: <input type="text" name="p" value="" onkeyup="calcolo()"><br>***

***Inserisci <i>q</i>: <input type="text" name="q" value="" onkeyup="calcolo()"><br>***

***N = <i>p</i> \* <i>q</i> = <SPAN ID="n">0</SPAN><br>***

***&#216 = (<i>p</i>-1)\*(<i>q</i>-1) = <SPAN ID="pp">0</SPAN> \* <SPAN ID="qq">0</SPAN> = <SPAN ID="o">0</SPAN><br>***

***Inserisci <i>e</i>: <input type="text" name="e" value=""> <input type="button" onClick="calcolad()" value="Calcola d"><br>***

***<br><center><SPAN ID="d"><b><i>spazio tabella per calcolo della d</i></b></SPAN></center><br>***

***Chiave pubblica = (e,N) = (<span id="se">0</span>,<span id="sn1">0</span>)<br>***

***Chiave privata = (d,N) = (<span id="sd">0</span>,<span id="sn2">0</span>)***

***<br><br>***

***</span>***

***</fieldset>***

***<br>***

***<fieldset>***

***<legend><div>Cifratura di un messaggio</div></legend>***

***<span>***

***Inserisci e: <input type="text" name="em1" value=""><br>***

***Inserisci N: <input type="text" name="nm1" value=""><br>***

***Inserisci messaggio: <input type="text" name="m1" value="" size="60"><br>***

***<center><input type="button" onClick="pp()" value="Cifra" style="width:300px"></center><br>***

***<CENTER><span id="pr"></span>***

***</CENTER><br>***

***</SPAN>***

***</FIELDSET>***

***<BR>***

***<fieldset>***

***<legend><div>Decifratura di un messaggio</div></legend>***

***<span>***

***Inserisci d: <input type="text" name="dm2" value=""><br>***

***Inserisci N: <input type="text" name="nm2" value=""><br>***

***Inserisci messaggio (CODICI ASCII SEPARATI DA , ) :<br><input type="text" name="m2" value="" size="60"><BR><br>***

***<center><input type="button" onClick="pd()" value="Decifra" style="width:300px"></center><br>***

***<CENTER><span id="pr2"></span></CENTER><br>***

***</span>***

***</fieldset>***

***</form>***

***</CENTER>***

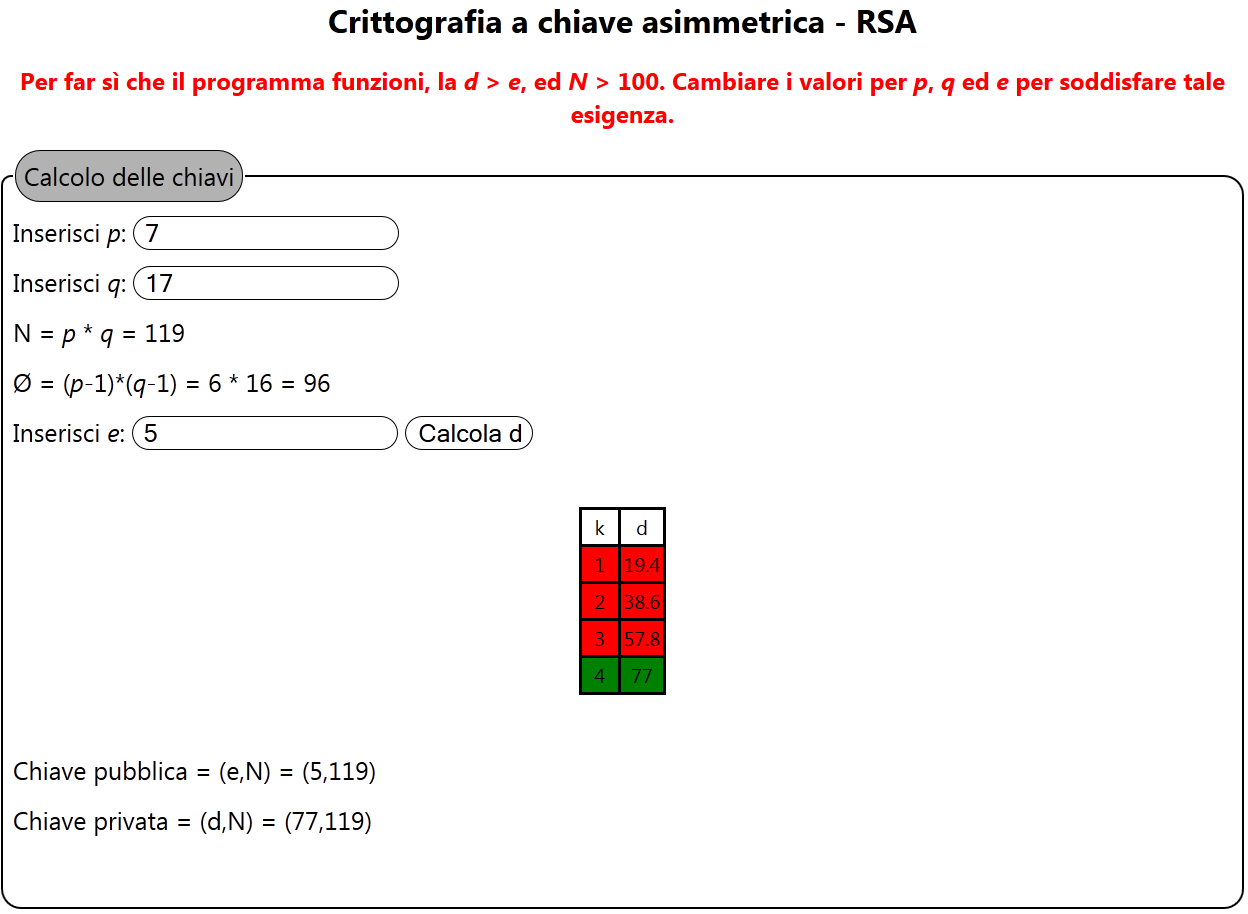
***</BODY>***

***</HTML>***

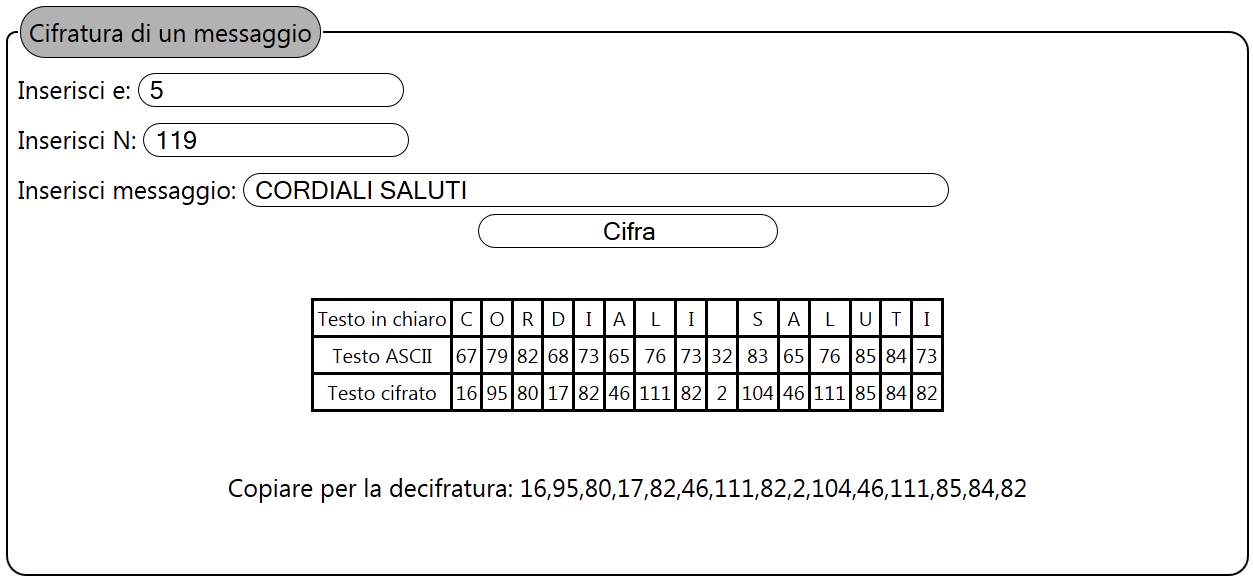
**Per testare il programma, visitare il sito:** [**www.lucapatera.altervista.org/SCUOLA/rsa**](http://www.lucapatera.altervista.org/SCUOLA/rsa)

**Simulazione del Sistema:**

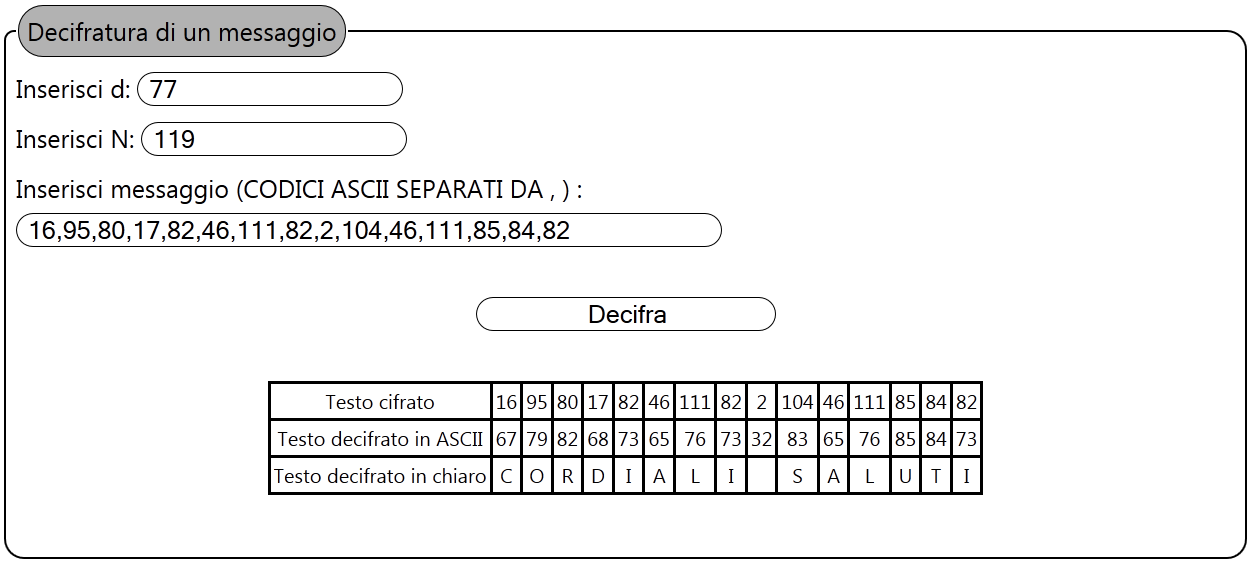
**Per il collaudo del sistema, useremo lo stesso esercizio del libro “Reti Telematiche” di A.C. Neve alla pag. 101:**

****

Come si nota inserendo i valori p, q ed e vengono calcolate le chiavi e visualizzati tutti i cicli per calcolare d.



Come si nota inserendo e ed N viene stampata una tabella in cui visualizza i valori di ogni passaggio effettuato.



La stessa cosa accade nella decifratura visualizzando correttamente tutti i passaggi effettuati.

**Commenti e impressioni:**

Notiamo che se d è minore di e ed N è minore di 100 il programma precedente non funzionerà a causa di una possibile ipotesi: se proviamo ad effettuare una di queste azioni sopra, nel programma, quando cifrerà il messaggio, ci si troverà in una situazione di qualche possibile zero e questo non deve accadere altrimenti alla decifratura sarà sempre 0 e quindi impossibile da convertire.

**Conclusioni:**

In questa esercitazione di laboratorio abbiamo visto come implementare un algoritmo per la Cifratura e decifratura dei messaggi tramite l’RSA, abbiamo incontrato qualche imprevisto spiegato precedentemente ma risolvibile grazie al fatto che l’algoritmo a chiave simmetrica deve utilizzare dei numeri primi molto grandi.

L’efficacia dell’RSA sta nel fatto che una funzione unidirezionale cioè che sarà molto difficile risalire al valore dei due numeri tramite il prodotto.

Tutto ciò rende praticamente impossibile risalire al valore della chiave privata conoscendo la chiave pubblica grazie all’utilizzo della funzione unidirezionale basata sull’aritmetica modulare.